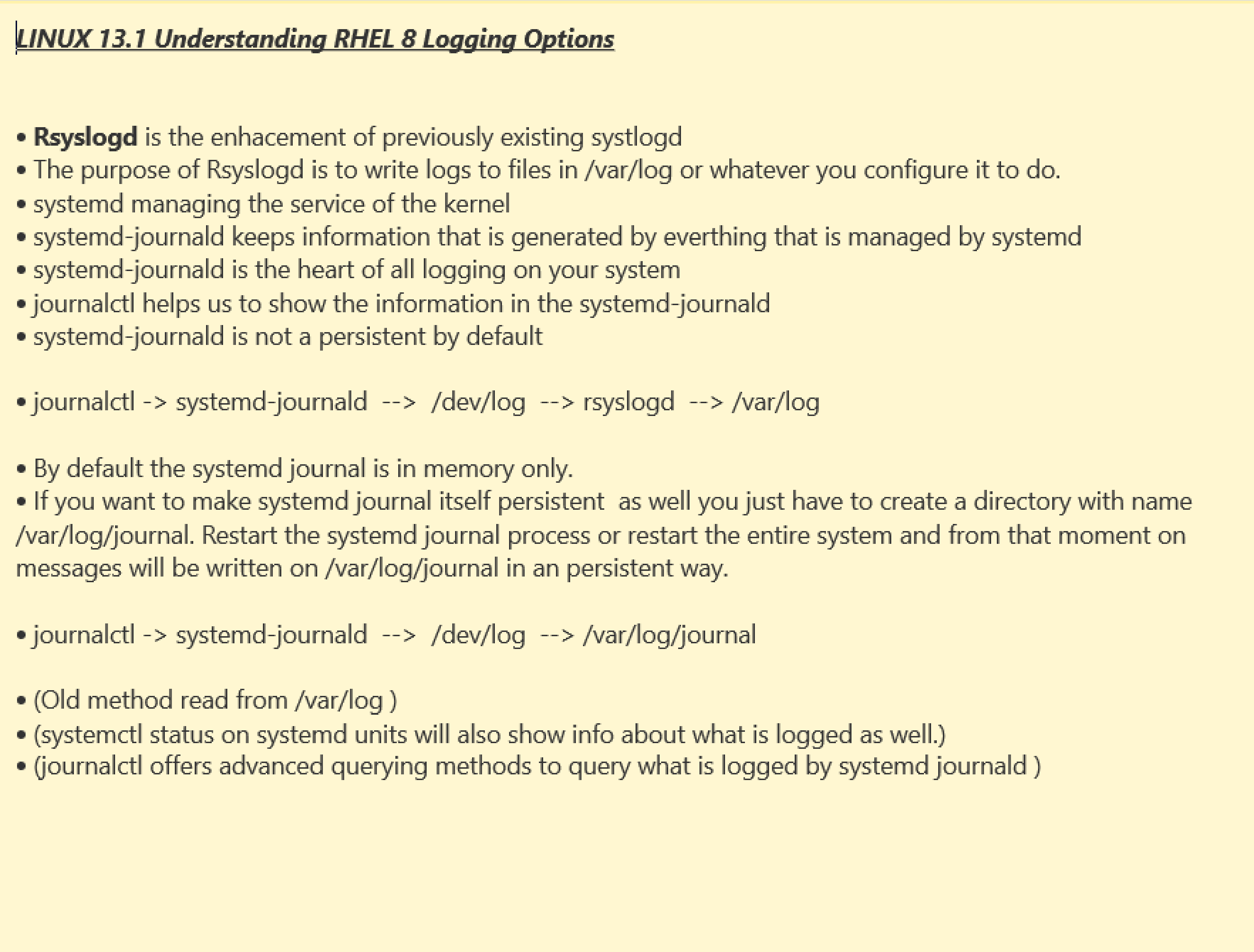
Chapter 13

By Etisha jain

Vishu Goyal



LINUX 13.1 Understanding RHEL 8 Logging Options

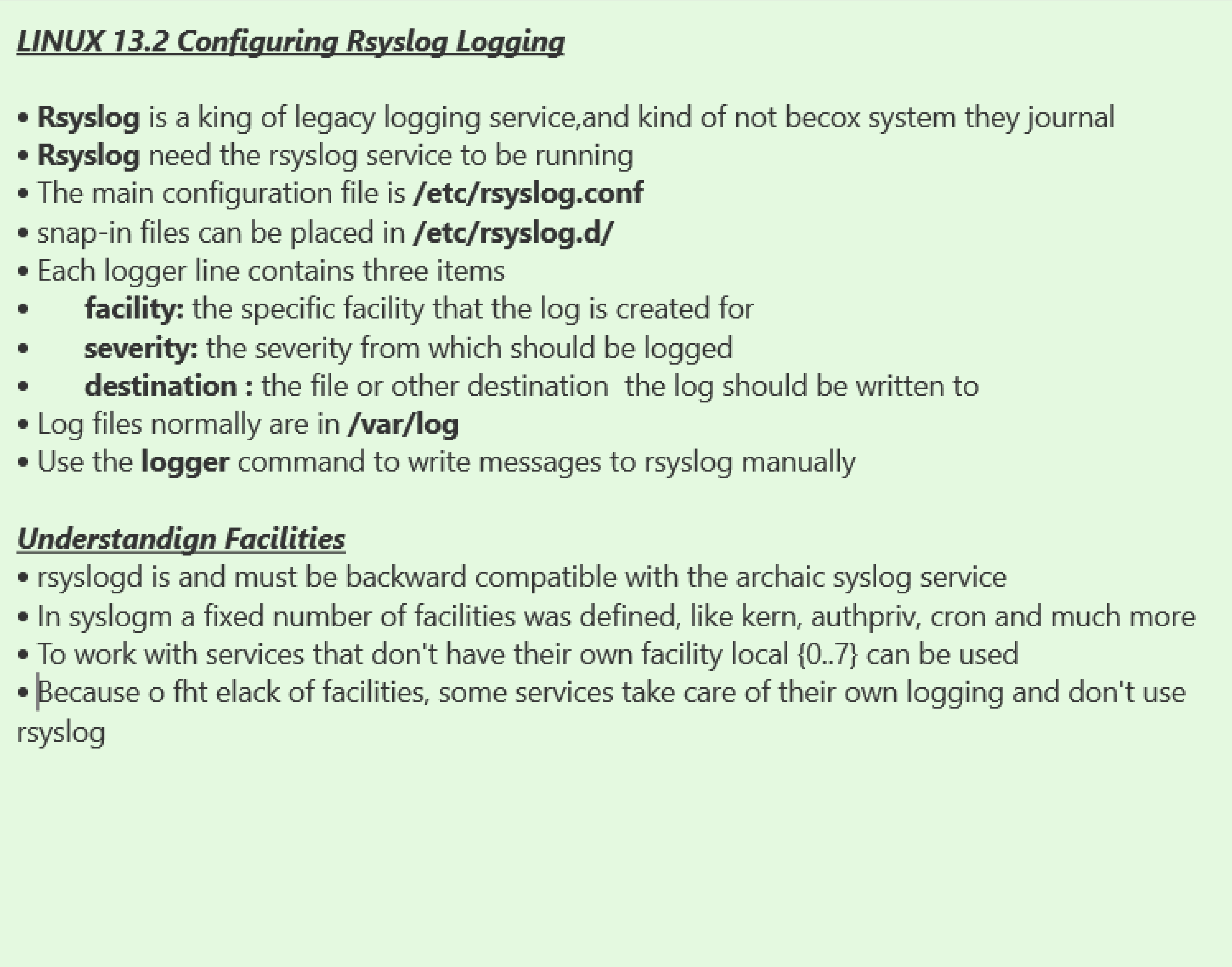
- **Rsyslogd** is the enhacement of previously existing systlogd
- The purpose of Rsyslogd is to write logs to files in /var/log or whatever you configure it to do.
- systemd managing the service of the kernel
- systemd-journald keeps information that is generated by everthing that is managed by systemd
- systemd-journald is the heart of all logging on your system
- journalctl helps us to show the information in the systemd-journald
- systemd-journald is not a persistent by default

- journalctl -> systemd-journald --> /dev/log --> rsyslogd --> /var/log

- By default the systemd journal is in memory only.
- If you want to make systemd journal itself persistent as well you just have to create a directory with name /var/log/journal. Restart the systemd journal process or restart the entire system and from that moment on messages will be written on /var/log/journal in an persistent way.

- journalctl -> systemd-journald --> /dev/log --> /var/log/journal

- (Old method read from /var/log)
- (systemctl status on systemd units will also show info about what is logged as well.)
- (journalctl offers advanced querying methods to query what is logged by systemd journald)



LINUX 13.2 Configuring Rsyslog Logging

- **Rsyslog** is a king of legacy logging service,and kind of not becox system they journal
- **Rsyslog** need the rsyslog service to be running
- The main configuration file is **/etc/rsyslog.conf**
- snap-in files can be placed in **/etc/rsyslog.d/**
- Each logger line contains three items
    - **facility:** the specific facility that the log is created for
    - **severity:** the severity from which should be logged
    - **destination :** the file or other destination the log should be written to
- Log files normally are in **/var/log**
- Use the **logger** command to write messages to rsyslog manually

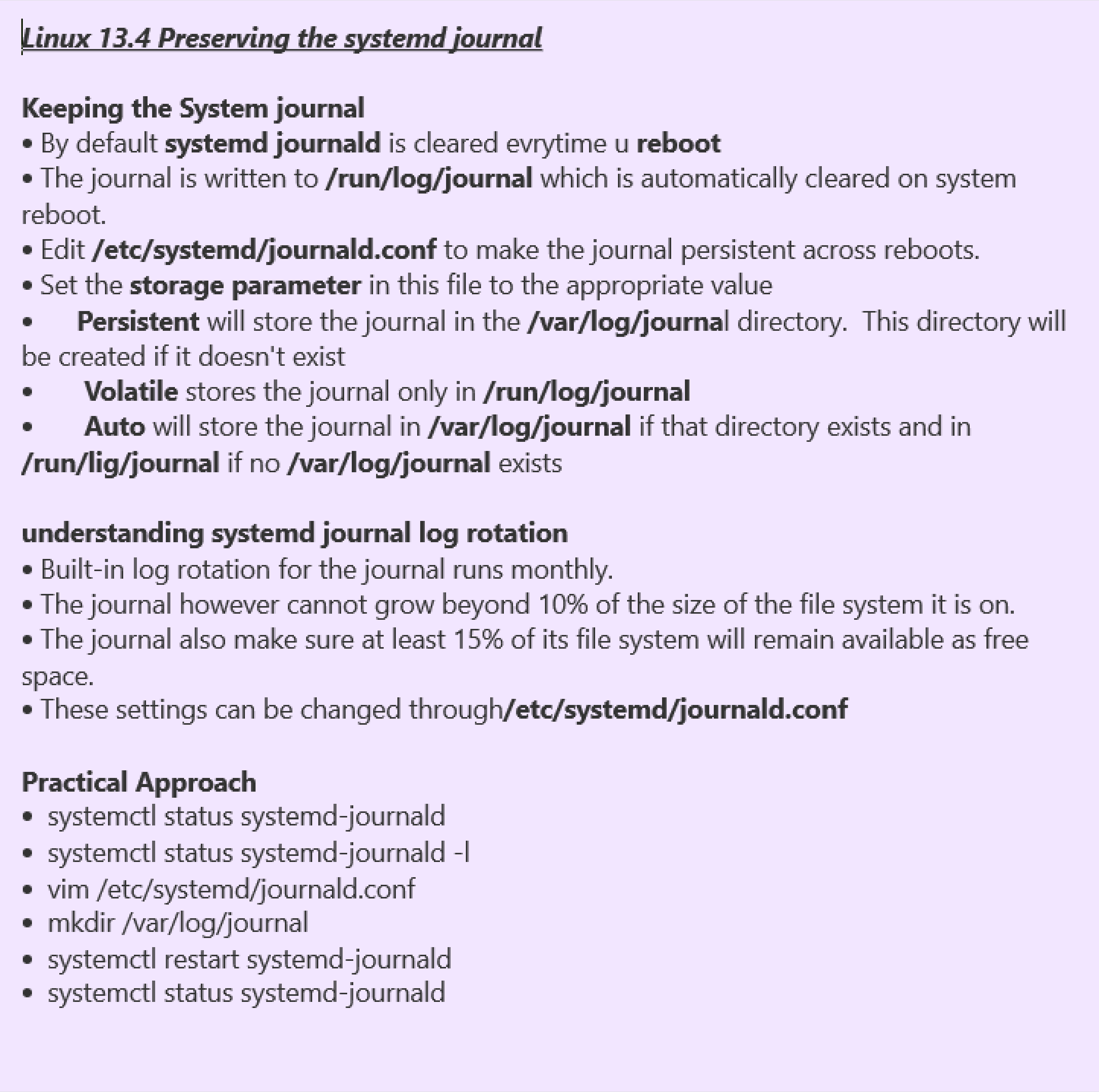
Understandign Facilities

- rsyslogd is and must be backward compatible with the archaic syslog service
- In syslogm a fixed number of facilities was defined, like kern, authpriv, cron and much more
- To work with services that don't have their own facility local {0..7} can be used
- Because o fht elack of facilities, some services take care of their own logging and don't use rsyslog

Linux 13.3 Working with systemd-journald

- **systemd-journald** is the log service that is a part of systemd(everything happening since the start of your system is logged).
- It integrates well with the **systemctl status <unit>** output(can see recent messages I.e. it makes log messages very accessible).
- Alternatively, the **journalctl** command can be used to read log entries in the journal.
- Messages are logged also to rsyslog using the rsyslogd **Imjournal** module
- To make the journal persistent (I.e. to keep log messages of before your system booting also)use **mkdir /var/log/journal**

- **mkdir /var/log/journal**
- **vim /etc/systemd/**
- **vim /etc/systemd/journald.conf**
- **journalctl** (get access to journal use D to scroll down arrow to right to see messages that are wrapped)
- **journalctl** tab completion
- **journalctl UNIT=sshd**
- **systemctl status httpd**



Linux 13.4 Preserving the systemd journal

Keeping the System journal

- By default **systemd journald** is cleared evrytime u **reboot**
- The journal is written to **/run/log/journal** which is automatically cleared on system reboot.
- Edit **/etc/systemd/journald.conf** to make the journal persistent across reboots.
- Set the **storage parameter** in this file to the appropriate value
- **Persistent** will store the journal in the **/var/log/journa**l directory. This directory will be created if it doesn't exist
- **Volatile** stores the journal only in **/run/log/journal**
- **Auto** will store the journal in **/var/log/journal** if that directory exists and in **/run/lig/journal** if no **/var/log/journal** exists

understanding systemd journal log rotation

- Built-in log rotation for the journal runs monthly.
- The journal however cannot grow beyond 10% of the size of the file system it is on.
- The journal also make sure at least 15% of its file system will remain available as free space.
- These settings can be changed through**/etc/systemd/journald.conf**

Practical Approach

- systemctl status systemd-journald
- systemctl status systemd-journald -l
- vim /etc/systemd/journald.conf
- mkdir /var/log/journal
- systemctl restart systemd-journald
- systemctl status systemd-journald

Linux 13.5 Configuring Logging

- **Logrotate** is started through cron.daily to ensure that log files don't grow too big
- Main configuration is in **/etc/logrotate.conf** , snap-in files can be provided through **/etc/logrotate.d/**

- **vim logrotate.conf**
- **cd logrotate.d/**
- **ls**
- **vim httpd**
- **cd ..**
- **cd logrotate.d/**
- **cd ../**
- **vim logrotate.conf**

Thank You